

## **COMMONWEALTH OF VIRGINIA**



# **Information Technology Resource Management Information Technology Security Standard**

**Virginia Information Technologies Agency (VITA)**

---

## ITRM PUBLICATION VERSION CONTROL

ITRM Publication Version Control: It is the User's responsibility to ensure they have the latest version of this ITRM publication. Questions should be directed to VITA's Associate Director for Policy Practice and Architecture (PPA) within the Technology Strategies and Solutions (TSS) Directorate. PPA will issue a Change Notice Alert and post on the VITA Web site, provide an email announcement to the Agency Information Technology Resources (AITRs) and Information Security Officers (ISOs) at all state agencies and institutions as well as other parties PPA considers to be interested in the change.

This chart contains a history of this ITRM publication's revisions.

Version	Date	Purpose of Revision
Original	12/07/2001	Base Document
Revision 1	07/01/2006	To update all sections of the Standard in accordance with changes to the <i>Code of Virginia</i> as well as incorporate emerging best practices.

---

---

## PREFACE

***Publication Designation***

ITRM Standard SEC501-01

***Subject***

Information Technology Security

***Effective Date***

July 1, 2006

***Compliance Date***

July 1, 2007

***Supersedes***

COV ITRM Standard SEC2001-01.1 Information Technology Security, dated December 7, 2001

***Scheduled Review***

One (1) year from effective date

***Authority***

*Code of Virginia* § 2.2-603(G)  
(Authority of Agency Directors)

*Code of Virginia*, §§ 2.2-2005 – 2.2-2032.  
(Creation of the Virginia Information Technologies Agency; “VITA;” Appointment of Chief Information Officer (CIO))

*Code of Virginia*, § 2.2-2009  
(Additional Powers of the CIO relating to security)

*Code of Virginia*, § 2.2-2827  
(Restrictions on State employee access to information Infrastructure)

*Code of Virginia*, § 2.2-3803  
(Administration of systems including personnel information; Internet privacy policy)

***Scope***

This *Standard* is applicable to all Executive Branch State Agencies and institutions of higher education (collectively referred to as “Agency”) that manage, develop, purchase, and use information technology resources in the Commonwealth. Academic “instruction or research” systems, however, are exempt from this *Standard*. This exemption, does not, however, relieve these Academic “instruction or research” systems from meeting the requirements of any other state or federal Law or Act to which they are subject. This *Standard* is offered only as guidance to local government entities. Exceptions from the applicability of this *Standard* are defined in detail in Section 1.6.

***Purpose***

To define the minimum requirements for each Agency’s information technology security management program.

***General Responsibilities***

*(Italics indicate quote from the Code of Virginia requirements)*

***Chief Information Officer***

In accordance with *Code of Virginia* § 2.2-2009, the Chief Information Officer (CIO) is assigned the following duties: “*the CIO shall direct the development of policies, procedures and standards for assessing security risks, determining the appropriate security measures and performing security audits of government databases and data communications. At a minimum, these policies, procedures, and standards shall address the scope of security audits and which public bodies are authorized to conduct security audits.*”

***Chief Information Security Officer***

The Chief Information Officer (CIO) has designated the Chief Information Security Officer (CISO) to develop Information Security policies, procedures, and standards to protect the confidentiality, integrity, and availability of the Commonwealth of Virginia’s information technology systems and data.

***Council on Technology Services***

In accordance with the *Code of Virginia* § 2.2-2009, the Council on Technology Services is assigned the following duties: “*In developing and updating such policies, procedures and standards, the CIO shall consider, at a minimum, the advice and recommendations of the Council on Technology Services.*”

***Technology Strategies and Solutions Directorate***

In accordance with the *Code of Virginia* § 2.2-2010, the CIO has assigned the Technology Strategies and Solutions Directorate the following duties: *Develop and adopt policies, standards, and guidelines for managing information technology by state agencies and institutions.*”

***All State Agencies***

In accordance with § 2.2-603, § 2.2-2009 and § 2.2-2005, all Executive Branch State Agencies are responsible for complying with all Commonwealth

---

ITRM policies and standards, and considering Commonwealth ITRM guidelines issued by the Chief Information Officer of the Commonwealth. In addition: *“The director of every department in the executive branch of state government shall report to the Chief Information Officer as described in § 2.2-2005, all known incidents that threaten the security of the Commonwealth's databases and data communications resulting in exposure of data protected by federal or state laws, or other incidents compromising the security of the Commonwealth's information technology systems with the potential to cause major disruption to normal Agency activities. Such reports shall be made to the Chief Information Officer within 24 hours from when the department discovered or should have discovered their occurrence.”*

### ***Regulatory References***

1. Health Insurance Portability and Accountability Act
2. Privacy Act of 1974
3. Children's Online Privacy Protection Act
4. Family Educational Rights and Privacy Act
5. Executive Order of Critical Infrastructure Protection
6. Federal Child Pornography Statute: 18 U.S.C. & 2252
7. Federal Rehabilitation Act of 1973, § 508
8. Bank Secrecy Act
9. Virginia Computer Crime Act, *Code of Virginia*, §18.2-152.3.,4., 5., and 6
10. Library of Virginia Records Management Program, *Code of Virginia*, Title 42.1, Chapter 7, sec 42.1-85
11. Federal Information Security Management Act (FISMA)
12. Office of Management and Budget (OMB) Circular A-130

### ***International Standards***

1. International Standard, Information Technology – code of practice for information security management, BS ISO/IEC 17799:2005.

### ***Definitions***

See [Glossary](#)

### ***Related ITRM Policy***

ITRM Policy SEC500-02: Information Security Management Policy (Revised 07/01/2006)

# TABLE OF CONTENTS

ITRM PUBLICATION VERSION CONTROL.....	ii
PREFACE .....	iii
1. INTRODUCTION .....	1
1.1 Intent .....	1
1.2 Organization of this Standard .....	1
1.3 Roles and Responsibilities .....	2
1.4 IT Security Policy and Program.....	2
1.5 Exceptions to Security Requirements .....	2
1.6 Exemptions from Applicability.....	2
2. RISK MANAGEMENT.....	3
2.1 Purpose.....	3
2.2 IT Security Roles and Responsibilities .....	3
2.2.1 Purpose .....	3
2.2.2 Requirements.....	3
2.3 Business Impact Analysis .....	4
2.3.1 Purpose .....	4
2.3.2 Requirements.....	4
2.4 IT System and Data Sensitivity Classification.....	5
2.4.1 Purpose .....	5
2.4.2 Requirements.....	5
2.5 IT System Inventory and Definition .....	6
2.5.1 Purpose .....	6
2.5.2 Requirements.....	6
2.6 Risk Assessment .....	6
2.6.1 Purpose .....	6
2.6.2 Requirements.....	7
2.7 IT Security Audits.....	7
2.7.1 Purpose .....	7
2.7.2 Requirements.....	7
3. IT CONTINGENCY PLANNING .....	8
3.1 Purpose.....	8
3.2 Continuity of Operations Planning .....	8
3.2.1 Purpose .....	8
3.2.2 Requirements.....	8
3.3 IT Disaster Recovery Planning .....	9
3.3.1 Purpose .....	9
3.3.2 Requirements.....	9
3.4 IT System and Data Backup and Restoration .....	9
3.4.1 Purpose .....	9
3.4.2 Requirements.....	9
4. IT SYSTEMS SECURITY .....	10
4.1 Purpose.....	10
4.2 IT System Hardening .....	10
4.2.1 Purpose .....	10

---

4.2.2	<i>Requirements</i> .....	10
4.3	IT Systems Interoperability Security .....	10
4.3.1	<i>Purpose</i> .....	10
4.3.2	<i>Requirements</i> .....	11
4.4	Malicious Code Protection.....	11
4.4.1	<i>Purpose</i> .....	11
4.4.2	<i>Requirements</i> .....	11
4.5	IT Systems Development Life Cycle Security.....	13
4.5.1	<i>Purpose</i> .....	13
4.5.2	<i>Requirements</i> .....	13
5.	LOGICAL ACCESS CONTROL .....	15
5.1	Purpose.....	15
5.2	Account Management .....	15
5.2.1	<i>Purpose</i> .....	15
5.2.2	<i>Requirements</i> .....	15
5.3	Password Management .....	16
5.3.1	<i>Purpose</i> .....	16
5.3.2	<i>Requirements</i> .....	16
5.4	Remote Access.....	17
5.4.1	<i>Purpose</i> .....	17
5.5.2	<i>Requirements</i> .....	17
6.	DATA PROTECTION.....	18
6.1	Purpose.....	18
6.2	Data Storage Media Protection .....	18
6.2.1	<i>Purpose</i> .....	18
6.2.2	<i>Requirements</i> .....	18
6.3	Encryption.....	18
6.3.1	<i>Purpose</i> .....	18
6.3.2	<i>Requirements</i> .....	19
7.	FACILITIES SECURITY.....	20
7.1	Purpose.....	20
7.2	Requirements .....	20
8.	PERSONNEL SECURITY .....	21
8.1	Purpose.....	21
8.2	Access Determination and Control .....	21
8.2.1	<i>Purpose</i> .....	21
8.2.2	<i>Requirements</i> .....	21
8.3	IT Security Awareness and Training .....	22
8.3.1	<i>Purpose</i> .....	22
8.3.2	<i>Requirements</i> .....	22
8.4	Acceptable Use .....	23
8.4.1	<i>Purpose</i> .....	23
8.4.2	<i>Requirements</i> .....	23
9.	THREAT MANAGEMENT.....	24
9.1	Purpose.....	24
9.2	Threat Detection.....	24
9.2.1	<i>Purpose</i> .....	24

---

9.2.2	<i>Requirements</i> .....	24
9.3	Incident Handling.....	24
9.3.1	<i>Purpose</i> .....	24
9.3.2	<i>Requirements</i> .....	24
9.4	IT Security Monitoring and Logging.....	25
9.4.1	<i>Purpose</i> .....	25
9.4.2	<i>Requirements</i> .....	25
10.	IT ASSET MANAGEMENT.....	27
10.1	Purpose.....	27
10.2	IT Asset Control.....	27
10.2.1	<i>Purpose</i> .....	27
10.2.2	<i>Requirements</i> .....	27
10.3	Software License Management.....	27
10.3.1	<i>Purpose</i> .....	27
10.3.2	<i>Requirements</i> .....	27
10.4	Configuration Management and Change Control .....	27
10.4.1	<i>Purpose</i> .....	27
10.4.3	<i>Requirements</i> .....	28
	GLOSSARY OF IT SECURITY DEFINITIONS .....	30
	IT SECURITY ACRONYMS.....	36
	APPENDIX – IT SECURITY POLICY AND STANDARD EXCEPTION REQUEST FORM	37

---

## 1. INTRODUCTION

### 1.1 Intent

The intent of the *Information Technology Security Standard* is to establish a baseline of information technology (IT) security controls that include, but are not limited to, the requirements of all statutes and best practices listed on pages iii and iv. These controls will provide protection of Commonwealth of Virginia (COV) IT systems and data.

This *Standard* defines the minimum acceptable level of IT security for the COV, and Agencies must implement an IT security program that complies with this *Standard*. Agencies may implement their own IT security standards, based on IT security needs specific to their environments and commensurate with sensitivity and risk; Agency IT security standards, however, must provide protection of the Agency's IT systems and data equal to or greater than the requirements defined in this document. As used in this *Standard*, sensitivity encompasses the elements of confidentiality, integrity, and availability. See Section 2.5 for additional detail on sensitivity.

The COV IT Security Program consists of the following set of components:

- Risk Management
- IT Contingency Planning
- IT Systems Security
- Logical Access Control
- Data Protection
- Facilities Security
- Personnel Security
- Threat Management
- IT Asset Management

These components provide a framework to allow state Agencies to accomplish their missions in a safe and secure technology environment. In addition, they provide a basis for each Agency's IT security program. Each component listed above contains requirements that, together, comprise this *Information Technology Security Standard*.

This *Standard* recognizes that Agencies may procure IT equipment, systems, and services covered by this *Standard* from third parties. In such instances, Agency Heads remain accountable for maintaining compliance with this *Standard* and Agencies must enforce these compliance requirements through documented agreements with third-party providers. Similarly, VITA customer Agencies must provide VITA with information concerning their IT security requirements to enable VITA to meet the requirements of this *Standard* on their behalf.

### 1.2 Organization of this *Standard*

The nine components of the COV IT Security Program (listed in section 1.1, above) provide the organizational framework for this *Standard*. Each component consists of one or more sections composed of:

- A **Purpose** statement that provides a high-level description of the component or subcomponent and its importance in the COV IT Security Program;
- **Requirements**, which describe mandatory technical or programmatic activities in detail for a specific area of the COV IT Security Program;



- **Notes**, which provide guidance and explanation regarding the requirements; and
- **Examples**, which describe ways in which Agencies might meet the requirements. These examples do not and should not be interpreted to suggest an appropriate course of action for particular COV agencies, personnel, systems, or facilities.

### 1.3 Roles and Responsibilities

Descriptions of key IT security roles and responsibilities are included in the *Information Technology Security Policy* (COV ITRM Policy SEC501-02). These roles and responsibilities are also contained in the Glossary of this *Standard*.

### 1.4 IT Security Policy and Program

Each Agency shall establish, document, implement, and maintain its IT security program appropriate to its business and technology environment in compliance with this *Standard*. In addition, because resources that can reasonably be committed to protecting IT systems are limited, each Agency must implement its IT security program in a manner commensurate with sensitivity and risk.

### 1.5 Exceptions to Security Requirements

The Chief Information Security Officer of the Commonwealth (CISO) must approve exceptions to this Standard. For each exception, the requesting Agency shall document:

- The business need,
- The scope and extent,
- Mitigating safeguards,
- The specific duration, and
- Agency Head approval.

If the CISO denies a request for an exception to this *Standard*, the Agency requesting the exception may appeal the denial to the Chief Information Officer of the Commonwealth (CIO) through the CISO. The form that Agencies must use to document such exception requests is included as the Appendix to this document.

### 1.6 Exemptions from Applicability

The following are explicitly exempt from complying with the requirements defined in this document:

- a. Systems under development and/or experimental systems that do not create additional risk to production systems
- b. Surplus and retired systems
- c. Academic instruction or research systems (This exemption, however, does not relieve these academic instruction or research systems from meeting the requirements of any other state or federal Law or Act to which they are subject.)

## 2. RISK MANAGEMENT

### 2.1 Purpose

Risk Management delineates the steps necessary to identify, analyze, prioritize, and mitigate risks that could compromise COV IT systems. This section defines requirements in the following areas:

- IT Security Roles and Responsibilities
- IT System Inventory and Definition
- Business Impact Analysis
- IT System and Data Sensitivity Classification
- Risk Assessment
- IT Security Audits
- Risk Response

### 2.2 IT Security Roles and Responsibilities

#### 2.2.1 Purpose

IT Security Roles and Responsibilities requirements identify the steps necessary to establish formal roles and assign responsibilities to manage and protect the security of COV IT systems, as required by the *Information Technology Security Policy* (COV ITRM Policy SEC500-02).

#### 2.2.2 Requirements

Each Agency Head shall fulfill the following responsibilities:

1. As required by Section 2.3 of the *COV IT Security Policy* (ITRM Policy SEC500-02), via e-mail to [VITASecurityServices@vita.virginia.gov](mailto:VITASecurityServices@vita.virginia.gov), designate an Information Security Officer (ISO) for the agency, and provide the person's name, title and contact information to VITA no less than biennially. The Agency Head is strongly encouraged to designate at least one backup for the ISO.

Each Agency Head or designated ISO shall fulfill the following responsibilities:

1. Assign individuals to the roles described in the *COV Information Technology Security Policy* (ITRM Policy SEC500-02).

**Note:** See the *Information Technology Security Policy* (ITRM Policy SEC500-02) for a further discussion of responsibilities associated with these roles. Roles and their associated responsibilities are also contained in the Glossary.

2. Document the responsibilities of the designee for each role identified.
3. Prevent conflict of interests and adhere to the security concept of separation of duties by assigning roles so that:
  - a. The ISO is not a System Owner or a Data Owner;
  - b. The System Owner and the Data Owner are not System Administrator for systems or data they own; and
  - c. The ISO, System Owners, and Data Owners are COV employees.

**Notes:**

- Other roles can be assigned to contractors. For roles assigned to contractors, the contract language shall include specific responsibility and background check requirements.
- The System Owner can own multiple systems.
- Data Owners can own data on multiple systems.
- System Administrators can assume responsibility for multiple systems.

## **2.3 Business Impact Analysis**

### **2.3.1 Purpose**

Business Impact Analysis (BIA) delineates the steps necessary for Agencies to identify their business functions, identify those Agency business functions that are essential to an Agency's mission, and identify the resources that are required to support these essential Agency business functions.

**Note:** The requirements below address only the IT aspects of BIA. Agencies should consult the *COOP Planning Manual* published by the Virginia Department of Emergency Management (VDEM) for non-IT related BIA requirements.

### **2.3.2 Requirements**

Each Agency shall fulfill the following responsibilities:

1. Identify Agency business functions.
2. Identify primary essential business functions.

**Note:** A business function is essential if disruption or degradation of the function prevents the Agency from performing its mission, as described in the Agency mission statement.

3. Identify those secondary functions on which each essential function depends.

**Note:** Essential functions may depend upon functions not previously identified as essential and upon functions within and outside the Agency.

4. Determine the required recovery time for each primary and secondary essential business function, based on Agency and COV goals and objectives.
5. Identify the resources that support each primary and secondary essential business function.
6. For IT systems and/or data that support a primary or secondary essential business function, specify to what extent the essential business function depends upon the specific IT system and/or data.
7. Produce a BIA report for which the IT component:
  - a. Documents the dependence of the Agency's primary and secondary essential business functions on specific IT systems and/or data; and
  - b. Specifies the required recovery time for the IT systems and/or data on which a primary or secondary essential business function depends, based on:

- i. Agency and COV goals and objectives; and
  - ii. The extent to which an essential business function depends upon the IT systems and/or data.
8. Use the IT information documented in the BIA report as a primary input to IT System and Data Sensitivity Classification (Section 2.5), Risk Assessment (Section 2.6), and IT Contingency Planning (Section 3).
9. Conduct periodic review and revision of the Agency BIA, as needed, but at least once every three years.

## 2.4 IT System and Data Sensitivity Classification

### 2.4.1 Purpose

IT System and Data Sensitivity Classification requirements identify the steps necessary to classify IT systems and data according to their sensitivity with respect to the following three criteria:

- Confidentiality, which addresses sensitivity to unauthorized disclosure;
- Integrity, which addresses sensitivity to unauthorized modification; and
- Availability, which addresses sensitivity to outages.

Sensitive Data is any data of which the compromise with respect to confidentiality, integrity, and/or availability could adversely affect COV interests, the conduct of Agency programs, or the privacy to which individuals are entitled. Sensitive IT Systems are COV IT systems that store, process, or transmit sensitive data.

### 2.4.2 Requirements

Each Agency Data Owner shall fulfill the following responsibilities:

1. Identify the type(s) of data handled by each Agency IT system.
2. Determine whether each type of data is also subject to other regulatory requirements.

**Example:** Some COV systems may handle data subject to regulations such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA); the Privacy Act of 1974; the Rehabilitation Act of 1973, § 508, or Federal National Security Standards.

3. Determine the potential damages to the Agency of a compromise of confidentiality, integrity or availability of each type of data handled by the IT system, and classify the sensitivity of the data accordingly.

**Example:** Data Owners should construct a table similar to the following table. Data Owners must classify sensitivity requirements of all types of data. The following table is only an illustration.

System ID: ABC123	Sensitivity Criteria		
Type of Data	Confidentiality	Integrity	Availability
HR Policies	Low	High	Moderate
Medical Records	High	High	High
Criminal Records	High	High	High

Table 1: Sample Sensitivity Analysis Results

4. Classify the IT system as sensitive if any type of data handled by the IT system has a sensitivity of high on any of the criteria of confidentiality, integrity, or availability.

**Note:** Agencies should consider classifying systems as sensitive even if a type of data handled by the IT system has a sensitivity of moderate on the criteria of confidentiality, integrity, and availability.

5. Use the information documented in the sensitivity classification as a primary input to the Risk Assessment process (Section 2.6).

## 2.5 IT System Inventory and Definition

### 2.5.1 Purpose

IT System Inventory and Definition requirements identify the steps in listing and marking the boundaries of sensitive IT in order to provide cost-effective, risk-based security protection for IT systems, for the Agency as a whole, and for the COV enterprise.

### 2.5.2 Requirements

Each Agency shall fulfill the following responsibilities:

1. Conduct an inventory of all sensitive IT systems owned by the Agency and update the inventory as changes occur.

**Note:** Where more than one Agency may own the IT system, and the Agency or Agencies cannot reach consensus on which should serve as System Owner for the purposes of this *Standard*, upon request, the CIO of the Commonwealth will determine the System Owner.

2. Assign a System Owner, Data Owner(s), and System Administrator(s) for each Agency-owned sensitive IT system.

**Note:** A sensitive IT system may have multiple Data Owners, and/or System Administrators, but must have a single System Owner.

3. Document each sensitive IT system owned by the Agency, including its boundaries.

## 2.6 Risk Assessment

### 2.6.1 Purpose

Risk Assessment requirements delineate the steps Agencies must take for each system classified as sensitive to:

- Identify potential threats to an IT system and the environment in which it operates;
- Determine the likelihood that threats will materialize;
- Identify and evaluate vulnerabilities; and
- Determine the loss impact if one or more vulnerabilities are exploited by a potential threat.

**Note:** The Risk Assessment (RA) required by this *Standard* differs from the RA required by the COV *Project Management Standard* (ITRM Standard GOV2004-02.3.2). This *Standard* requires an RA based on operational risk, while the *Project Management Standard* requires an RA based on

project risk. Many of the RA techniques described in the *Project Management Standard*, however, may also be applicable to the RA required by this *Standard*.

### **2.6.2 Requirements**

For each Agency-owned IT system classified as sensitive, the Agency shall fulfill the following responsibilities:

1. Conduct a formal RA of the IT system, as needed, but not less than once every three years.
2. Conduct an annual self-assessment to determine the continued validity of the formal RA.

**Note:** In addition, in Agencies that own both sensitive IT systems and systems that are exempt from the requirements of this *Standard*, the Agency's RAs must include consideration of the added risk to sensitive systems from the exempt systems.

3. Prepare a report of each RA that includes, at a minimum, identification of all vulnerabilities discovered during the assessment, and an executive summary, including major findings and risk mitigation recommendations.

## **2.7 IT Security Audits**

### **2.7.1 Purpose**

IT Security Audit requirements define the steps necessary to assess whether IT security controls implemented to mitigate risks are adequate and effective.

### **2.7.2 Requirements**

For each Agency-owned IT system classified as sensitive, the Agency shall fulfill the following responsibilities:

1. Require that the IT system undergo an IT Security Audit as required by and in accordance with the *IT Security Audit Standard* (COV ITRM Standard SEC507-00).
2. Assign an individual to be responsible for managing IT Security Audits.

---

### 3. IT CONTINGENCY PLANNING

#### 3.1 Purpose

IT Contingency Planning delineates the steps necessary to plan for and execute recovery and restoration of COV IT systems and data if an event occurs that renders the systems and/or data unavailable. This component of the COV IT Security Program defines requirements in the following three areas:

- Continuity of Operations Planning
- Disaster Recovery Planning
- IT System Backup and Restoration

#### 3.2 Continuity of Operations Planning

##### 3.2.1 Purpose

COV Continuity of Operations Planning requirements are defined by VDEM. This section addresses only the Continuity of Operations Planning requirements for IT systems and data. Agencies should consult the *Continuity of Operations Planning Manual* published by VDEM for non-IT related requirements that address all essential business functions.

These Continuity of Operations Planning requirements identify the steps necessary to provide continuity for essential Agency IT systems and data through the development, implementation, exercise, and maintenance of the IT component of Continuity of Operations Plans.

##### 3.2.2 Requirements

Each Agency shall fulfill the following responsibilities:

1. Designate an employee to collaborate with the Agency Continuity of Operations Plan (COOP) coordinator as the focal point for IT aspects of COOP and related Disaster Recovery planning activities.

**Note:** Designation of an Agency COOP coordinator is included in the COOP planning requirements issued by VDEM.

2. Based on BIA and RA results, develop Agency COOP IT-related documentation which identifies:
  - a. Essential business functions that require restoration and the Recovery Time Objective (RTO) for each;
  - b. Recovery requirements for IT systems and data needed to support the essential business functions; and
  - c. Personnel contact information and incident notification procedures.

**Note:** The COOP should be protected as sensitive data and stored at a secure off-site location.

3. Require an annual exercise (or more often as necessary) of IT COOP components to assess their adequacy and effectiveness.
4. Require review and revision of IT COOP components following the exercise (and at other times as necessary).

### **3.3 IT Disaster Recovery Planning**

#### **3.3.1 Purpose**

IT Disaster Recovery Planning is the component of Continuity of Operations Planning that identifies the steps necessary to provide for restoring essential business functions on a schedule that supports Agency mission requirements. These steps lead to the creation of an IT Disaster Recovery Plan (DRP).

#### **3.3.2 Requirements**

Each Agency shall fulfill the following responsibilities:

1. Based on the COOP, develop and maintain an IT DRP, which supports the restoration of essential business functions.
2. Require approval of the IT DRP by the Agency Head.
3. Require periodic review, reassessment, testing, and revision of the IT DRP to reflect changes in essential business functions, services, system hardware and software, and personnel.
4. Require training of all IT Disaster Recovery team members as part of the Agency's IT security training program.
5. Establish communication methods to support IT system users' local and remote access to systems, as necessary.

### **3.4 IT System and Data Backup and Restoration**

#### **3.4.1 Purpose**

IT System and Data Backup and Restoration requirements identify the steps necessary to protect the availability and integrity of COV data documented in backup and restoration plans.

#### **3.4.2 Requirements**

For every IT system identified as sensitive, each Agency shall or shall require that its service provider implement backup and restoration plans to support restoration of systems and data in accordance with Agency requirements. At a minimum, these plans shall address the following:

1. Secure off-site storage for backup media
2. Performance of backups only by authorized personnel
3. Review of backup logs after the completion of each backup job to verify successful completion
4. Approval of backup schedules of a system by the System Owner
5. Approval of emergency backup and operations restoration plans by the System Owner
6. Protection of any backup media that is sent off site (physically or electronically), or shipped by the United States Postal Service or any commercial carrier, in accordance with Agency requirements



## 4. IT SYSTEMS SECURITY

### 4.1 Purpose

IT Systems Security requirements delineate steps to protect COV IT systems in the following four areas:

- IT System Hardening
- IT Systems Interoperability Security
- Malicious Code Protection
- IT Systems Development Life Cycle

### 4.2 IT System Hardening

#### 4.2.1 Purpose

IT System Hardening requirements delineate technical security controls to protect COV IT systems against IT security vulnerabilities.

#### 4.2.2 Requirements

Each Agency shall or shall require that its service provider fulfill the following responsibilities:

1. Identify, document, and apply appropriate baseline security configurations to Agency-owned IT systems, regardless of their sensitivity.
2. Identify, document, and apply more restrictive security configurations for sensitive Agency-owned IT systems, as necessary.

**Note:** Agencies may develop Agency-specific baseline security configuration standards or may elect to use baseline security configuration standards that are publicly available, such as those developed by the Center for Internet Security ([www.cisecurity.org](http://www.cisecurity.org)).

3. Maintain records that document the application of baseline security configurations.
4. Review and revise all security configuration standards annually, or more frequently, as needed.

**Note:** Agencies should establish a process to review and catalog applicable security notifications issued by equipment manufacturers, bulletin boards, security-related Web sites, and other security venues, and establish a process to update security baseline configuration standards based on those notifications.
5. Reapply all security configurations to Agency-owned IT systems, as appropriate, when the IT system undergoes a material change, such as an operating system upgrade.
6. Require periodic vulnerability scanning of IT systems in a manner commensurate with sensitivity and risk, to verify whether security configurations are in place and if they are functioning effectively.
7. Modify individual IT system configurations or baseline security configuration standards, as appropriate, to improve their effectiveness based on the results of vulnerability scanning.

### 4.3 IT Systems Interoperability Security

#### 4.3.1 Purpose

IT System Interoperability Security requirements identify steps to protect data shared with other IT systems.

### **4.3.2 Requirements**

For every sensitive Agency-owned IT system, the Agency shall or shall require that its service provider fulfill the following responsibilities by requiring that:

1. The System Owner, in consultation with the Data Owner, document IT systems with which data is shared. This documentation shall include:
  - a. The types of shared data;
  - b. The direction(s) of data flow; and
  - c. Contact information for the organization that owns the IT system with which data is shared, including the System Owner, the Information Security Officer (ISO), or equivalent, and the System Administrator.
2. The System Owners of the IT systems which share data develop a written agreement that delineates IT security requirements for each interconnected IT system and for each type of data shared.
3. The System Owners of the IT systems that share data inform one another regarding other IT systems with which their IT systems interconnect or share data, and inform one another prior to establishing any additional interconnections or data sharing.
4. The written agreement specify if and how the shared data will be stored on each IT system.
5. The written agreement specify that System Owners of the IT systems that share data acknowledge and agree to abide with any legal requirements regarding handling, protection, and disclosure of the shared data.
6. The written agreement maintain each Data Owner's authority to approve access to the shared data.
7. The System Owners approve and enforce the agreement.

## **4.4 Malicious Code Protection**

### **4.4.1 Purpose**

Malicious Code Protection requirements identify controls to protect IT systems from damage caused by malicious code.

### **4.4.2 Requirements**

Each Agency shall, or shall require that its service provider fulfill the following responsibilities:

1. Prohibit all IT system users from intentionally developing or experimenting with malicious programs (e.g., viruses, worms, spyware, keystroke loggers, phishing software, Trojan horses, etc.).
2. Prohibit all IT system users from knowingly propagating malicious programs including opening attachments from unknown sources.

3. Provide malicious program detection, protection, eradication, logging, and reporting capabilities.
4. Provide malicious code protection mechanisms on multiple IT systems and for all IT system users preferably deploying malicious code detection products from multiple vendors on various platforms.

**Example:** An Agency may elect to provide protection against malicious code transmitted via e-mail on the e-mail servers and on the desktop.

5. Require malicious program protection that:
  - a. Eliminates or quarantines malicious programs that it detects;
  - b. Provides an alert notification;
  - c. Automatically and periodically runs scans on memory and storage devices;
  - d. Automatically scans all files retrieved through a network connection, modem connection, or from an input storage device;
  - e. Allows only authorized personnel to modify program settings; and
  - f. Maintains a log of protection activities.
6. Provide the ability to eliminate or quarantine malicious programs in e-mail messages and file attachments as they attempt to enter the Agency's e-mail system.
7. Provide the ability for automatic download of definition files for malicious code protection programs whenever new files become available, and propagate the new files to all devices protected by the malicious code protection program.
8. Provide training on malicious code protection best practices to users as part of the IT security training program.
9. Require all forms of malicious code protection to start automatically upon system boot.
10. Provide network designs that allow malicious code to be detected and removed or quarantined before it can enter and infect a production device.
11. Provide procedures that instruct administrators and IT system users on how to respond to malicious program attacks, including shut-down, restoration, notification, and reporting requirements.
12. Require use of only new media (e.g. diskettes, CD-ROM) or sanitized media for making copies of software for distribution.
13. Prohibit the use of common use workstations and desktops (e.g., training rooms) to create distribution media.
14. By written policy, prohibit the installation of software on Agency IT systems until the software is approved by the Information Security Officer (ISO) or designee and, where practicable,

enforce this prohibition using automated software controls, such as Active Directory security policies.

## **4.5 IT Systems Development Life Cycle Security**

### **4.5.1 Purpose**

IT Systems Development Life Cycle Security requirements document the security-related activities that must occur in each phase of the development life cycle (from project definition through disposal) for Agency-owned IT application systems.

### **4.5.2 Requirements**

Each Agency shall fulfill the following responsibilities:

1. Incorporate IT security requirements in each phase of the life cycle, as well as for each modification proposed for the IT application system in each stage of its life cycle.

#### Project Initiation

2. Perform an initial risk analysis based on initial requirements and the business objectives to provide high-level security guidelines for the system developers.
3. Classify the types of data (see Section 2.4) that the IT system will process and the sensitivity of proposed IT system.
4. Assess the need for collection and maintenance of sensitive data before incorporating such collection and maintenance in IT system requirements.

#### Project Definition

5. Identify, develop, and document IT security requirements for the system during the Project Definition phase.
6. Incorporate IT security requirements in system design specifications.
7. Verify that the IT system development process designs, develops, and implements IT security controls that meet the IT security requirements in the design specifications.
8. Develop IT security evaluation procedures to validate that IT security controls developed for a new IT system are working properly and are effective.

**Note:** Some security controls (primarily those controls of a non-technical nature) cannot be tested and evaluated until after deployment of the IT system.

#### Implementation

9. Execute the IT security evaluation procedures to validate and verify that the functionality described in the specification is included in the product.

**Note:** Results should be documented in a report, including identification of controls that did not meet design specifications.

10. Conduct a RA (see Section 2.6) to assess the risk level of the IT application system.

11. Require that the system comply with all relevant Risk Management requirements in Section 2 of this document.

#### Disposition

12. Require retention of the data handled by an IT system in accordance with the Agency's records retention policy prior to disposing of the system.
13. Require that electronic media is sanitized prior to disposal, as documented in Section 6.2, so that all data is removed from the IT system.
14. Verify the disposal of hardware and software in accordance with the *COV Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard* (ITRM Standard SEC2003-02.1).

## **5. LOGICAL ACCESS CONTROL**

### **5.1 Purpose**

Logical Access Control requirements delineate the steps necessary to protect IT systems and data by verifying and validating that users are who they say they are and that they are permitted to use the IT systems and data they are attempting to access. This component of the COV IT Security Program defines requirements in the following three areas:

- Account Management
- Password Management
- Remote Access

### **5.2 Account Management**

#### **5.2.1 Purpose**

Account Management requirements identify those steps necessary to formalize the process of requesting, granting, administering, and terminating accounts.

#### **5.2.2 Requirements**

Each Agency shall or shall require that its service provider document formal account management practices for requesting, granting, administering, and terminating accounts. At a minimum, these practices shall include the following components:

1. Grant IT system users access to IT systems and data based on the principle of least privilege.
2. Require proper authorization and approval by the IT system user's supervisor and the System Owner to establish accounts.
3. Complete any Agency-required background check before establishing accounts, or as soon as practicable thereafter.
4. Provide for, at a minimum, annual review of all user accounts for sensitive IT system to assess the continued need for the accounts and access level and periodic review of user accounts for other IT systems.
5. Define authentication and authorization requirements, based on sensitivity and risk. Use of passwords on sensitive COV IT systems is required. Agencies should consider additional authentication methods, such as tokens and biometrics, based on sensitivity and risk.
6. Notify the System Administrator when IT system user accounts are no longer required, or when an IT system user's access level requirements change.
7. Prohibit the use of guest and shared accounts.
8. Lock an account automatically if it is not used for a predefined period.
9. Disable unneeded accounts.
10. Retain unneeded accounts in a disabled state in accordance with the Agency's records retention policy.

11. Associate access levels with group membership, where practicable, and require that every IT system user account be a member of at least one user group.
12. Notify supervisors, Human Resources, and the System Administrator in a timely manner about termination, transfer, or changes in access level requirements of IT system users.
13. Require that the System Owner and the System Administrator investigate any unusual IT system access activities and approve changes to access level authorizations.

### **5.3 Password Management**

#### **5.3.1 Purpose**

Password Management requirements specify the means for password use to protect systems and data.

#### **5.3.2 Requirements**

##### Account Passwords

Each Agency shall or shall require that its service provider document formal password management practices. At a minimum, these practices shall include the following components:

1. Require password use on all accounts on systems classified as sensitive, including local, remote access and temporary accounts. Agencies should consider whether sensitivity and risk require use of passwords on mobile devices such as cellular telephones and Personal Digital Assistants (PDAs).
2. Define requirements for password length and complexity based on sensitivity and risk.
3. Prohibit the transmission of identification and authentication data (e.g., passwords) without the use of industry accepted encryption standards (see Section 6.3 – Encryption).
4. Require IT system users to maintain exclusive control and use of their passwords, to protect them from inadvertent disclosure to others.
5. Configure sensitive IT systems to allow users to change their password at will.
6. Require users of sensitive IT systems to change their passwords after a pre-determined period (e.g., 90 days) as defined by the System Owner, based on sensitivity and risk.
7. Require that IT system users immediately change their passwords and notify the ISO if they suspect their passwords have been compromised.
8. Maintain password history files to prevent the reuse of the same or similar passwords, commensurate with sensitivity and risk.
9. Provide a unique initial password for each new user of sensitive IT systems, deliver the initial password to the IT system user in a secure and confidential manner, and require that the IT system user change the initial password upon the first login attempt.
10. Require that forgotten initial passwords be replaced rather than reissued.
11. Prohibit group account IDs and shared passwords on sensitive IT systems.

12. Prohibit the inclusion of passwords as plain text in scripts.
13. Limit access to files containing passwords to the IT system and its administrators.
14. Suppress the display of passwords on the screen as they are entered.
15. Determine requirements for hardware passwords based on sensitivity and risk
16. Document and store hardware passwords securely.
17. Implement procedures to handle lost or compromised passwords and/or tokens.
18. Require that System Administrators have both an administrative account and at least one user account and require that administrators use their administrative accounts only when performing tasks that require administrative privileges.
19. Require that at least two individuals have administrative accounts to each IT system, to provide continuity of operations.

## **5.4 Remote Access**

### **5.4.1 Purpose**

Remote Access requirements identify the steps necessary to provide for the secure uses of remote access within the COV enterprise network.

### **5.5.2 Requirements**

Commensurate with sensitivity and risk, each Agency shall or shall require that its service provider fulfill the following responsibilities:

1. Protect the security of all remote access to the Agency's sensitive IT systems and data by means of encryption, in a manner consistent with Section 6.3.  
  
**Note:** This encryption requirement applies both to session initiation (i.e., identification and authentication) and to all exchanges containing sensitive data.
2. Protect the security of remote file transfer of sensitive data to and from COV systems by means of encryption, in a manner consistent with Section 6.3.
3. Document requirements for use of remote access and for remote access to sensitive data.
4. Require that IT system users obtain formal authorization and a unique user ID and password prior to using the Agency's remote access capabilities.
5. Document requirements for the physical and logical hardening of remote access devices.
6. Require maintenance of auditable records of all remote access.
7. Provide training and instruction to IT system users on Agency remote access policies, standards, procedures, and guidelines prior to the users' receiving remote access capabilities.



## 6. DATA PROTECTION

### 6.1 Purpose

Data Protection requirements delineate the steps necessary to protect COV data from improper or unauthorized disclosure. This component of the COV IT Security Program defines requirements in the following two areas:

- Data Storage Media Protection
- Encryption

### 6.2 Data Storage Media Protection

#### 6.2.1 Purpose

Data Storage Media Protection requirements identify the steps necessary for the appropriate handling of stored data to protect the data from compromise.

#### 6.2.2 Requirements

Each Agency shall or shall require that its service provider document Data Storage Media protection practices. At a minimum, these practices must include the following components:

1. Define protection and identification of stored sensitive data as the responsibility of the creator or Data Custodian.
2. Require that sensitive data not be stored on mobile data storage media unless there is a documented agency business necessity approved in writing by the Agency Head and that all data storage media containing sensitive data be physically and logically secured.

**Note:** Such practices should apply to sensitive data stored on all data storage media, including removable data storage media and the fixed disk drives of all computer workstations, including mobile workstations such as laptop computers.

3. Restrict the pickup, receipt, transfer, and delivery of all data storage media containing sensitive data to authorized personnel.
4. Implement processes to sanitize data storage media prior to disposal or reuse.

**Note:** Agencies should implement procedures to instruct Administrators and users on the disposal of data storage media when no longer needed in accordance with the *ITRM Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard* (ITRM Standard SEC2003-02.1).

5. Include instructions in the Agency's IT security training program on the proper procedure for the disposal of data storage media containing sensitive.

### 6.3 Encryption

#### 6.3.1 Purpose

Encryption requirements provide a framework for selecting and implementing encryption controls to protect sensitive data.

**6.3.2 Requirements**

Commensurate with sensitivity and risk, each Agency shall fulfill the following responsibilities:

1. Define and document Agency practices for selecting and deploying encryption technologies and for the encryption of data.
2. Require training of users on the proper use of encryption products.
3. Document appropriate processes before implementing encryption. These processes must include the following components:
  - a. Instructions in the Agency's Incident Response Plan on how to respond when keys are compromised;
  - b. A secure key management system for the administration and distribution of encryption keys; and
  - c. Requirements to generate all encryption keys through an approved encryption package and securely store the keys in the event of key loss due to unexpected circumstances.

## **7. FACILITIES SECURITY**

### **7.1 Purpose**

Facilities Security requirements identify the steps necessary to safeguard the physical facilities that house COV IT equipment, systems, services, and personnel.

### **7.2 Requirements**

Commensurate with sensitivity and risk, each Agency shall or shall require that its service provider document facilities security practices. These practices must include the following components, at a minimum:

1. Safeguard IT systems and data residing in static facilities (such as buildings), mobile facilities (such as computers mounted in vehicles), and portable facilities (such as mobile command centers).
2. Design safeguards to protect against human, natural, and environmental risks.
3. Require appropriate environmental controls such as electric power, heating, fire suppression, ventilation, air-conditioning and air purification, as required by the IT systems and data.
4. Protect against physical access by unauthorized personnel.
5. Control physical access to essential computer hardware, wiring, displays, and networks by the principle of least privilege.
6. Provide a system of monitoring and auditing physical access to sensitive IT systems.

---

## 8. PERSONNEL SECURITY

### 8.1 Purpose

Personnel Security requirements delineate the steps necessary to restrict access to IT systems and data to those individuals who require such access as part of their job duties. This component of the COV IT Security Program defines requirements in the following three areas:

- Access Determination and Control
- Security Awareness and Training
- Acceptable Use

### 8.2 Access Determination and Control

#### 8.2.1 Purpose

Access Determination and Control requirements identify the steps necessary to restrict access to IT systems and data to authorized individuals.

#### 8.2.2 Requirements

Each Agency shall or shall require that its service provider document access determination and control practices for all sensitive Agency systems and all third-party systems with which sensitive Agency systems interconnect. At a minimum, these practices shall include the following components:

1. Perform background investigations of employees based on access to sensitive IT systems or data.

**Note:** Agencies should consult the *Code of Virginia* § 2.2-1201.1 and Department of Human Resource Management (DHRM) Policy 2.10.

2. Restrict visitor access to facilities that house sensitive COV IT systems or data.
3. Require non-disclosure and security agreements for access to IT systems and data, based on sensitivity and risk.
4. Remove physical and logical access rights upon personnel transfer or termination, or when requirements for access no longer exist, as required in Section 5.2 and Section 7.2.
5. Establish termination and transfer practices that require return of Agency logical and physical assets that provide access to sensitive COV IT systems and data and the facilities that house them.
6. Establish separation of duties in order to protect sensitive COV IT systems and data, or establish compensating controls when constraints or limitations of the Agency prohibit a complete separation of duties.

**Example:** Such compensating controls may include increased supervisory review; reduced span of control; rotation of assignments; independent review, monitoring, and/or auditing; and timed and specific access authorization with audit review, among others.

7. Explicitly grant physical and logical access to sensitive COV IT systems and data and the facilities that house them based on the principle of least privilege.

## 8.3 IT Security Awareness and Training

### 8.3.1 Purpose

Security Awareness and Training requirements identify the steps necessary to provide IT system managers, administrators, and users with awareness of system security requirements and of their responsibilities to protect COV IT systems and data.

### 8.3.2 Requirements

Each Agency shall fulfill the following responsibilities:

1. Designate an individual who is responsible for all aspects of an Agency's security awareness and training program including development, implementation, testing, training, monitoring attendance, and periodic updates.

**Note:** This responsibility is normally part of the ISO's role.

2. Include any Agency-specific IT security training requirements in the Agency IT security awareness and training program.

**Example:** An Agency that processes data covered by the Health Insurance Portability and Accountability Act (HIPAA) must have an IT security training program that addresses specific HIPAA data security requirements.

3. Require that all employees and contractors receive IT security awareness training annually, or more often as necessary.
4. Provide additional role-based IT security training commensurate with the level of expertise required for those employees and contractors who manage, administer, operate, and design IT systems, as practicable and necessary.

**Example:** Agency employees and contractors who are members of the Disaster Recovery Team or Incident Response Team require specialized training in these duties.

5. Implement processes to monitor and track attendance at IT security training.
6. Require IT security training before (or as soon as practicable after) IT system users receive access rights to the Agency's IT systems, and in order to maintain these access rights.
7. Develop an IT security training program so that each IT system user is aware of and understands the following concepts:
  - a. The Agency's policy for protecting IT systems and data, with a particular emphasis on sensitive systems and data;
  - b. The concept of separation of duties;
  - c. Employee responsibilities in continuity of operations, configuration management, and incident detection and reporting;
  - d. IT system user responsibilities and best practices in:
    - i. Prevention, detection, and eradication of malicious code;
    - ii. Proper disposal of data storage media; and
    - iii. Proper use of encryption products;

- e. Access controls, including creating and changing passwords and the need to keep them confidential;
  - f. Agency Remote Access policies; and
  - g. Intellectual property rights, including software licensing and copyright issues.
8. Require documentation of IT system users' acceptance of the Agency's security policies after receiving IT security training.

## 8.4 Acceptable Use

### 8.4.1 Purpose

Acceptable Use requirements identify the steps necessary to define acceptable and permitted use of COV IT systems.

### 8.4.2 Requirements

Each Agency shall or shall require that its service provider fulfill the following responsibilities:

1. Adhere to Virginia Department of Human Resource Management *Policy 1.75 – Use of Internet and Electronic Communication Systems*. Each Agency shall supplement the policy as necessary to address specific agency needs.

**Note:** This policy can be found at [http://www.dhrm.virginia.gov/hrpolicy/policy/pol1\\_75.pdf](http://www.dhrm.virginia.gov/hrpolicy/policy/pol1_75.pdf).

2. Inform IT system users that COV reserves the right (with or without cause) to monitor, access, and disclose all data created, sent, received, processed, or stored on COV systems.
3. Prevent users from:
  - a. Installing or using proprietary encryption hardware/software on COV systems;
  - b. Tampering with security controls configured on their workstations;
  - c. Installing personal software on a COV system;
  - d. Adding hardware to, removing hardware from, or modifying hardware on a COV system; and
  - e. Connecting unauthorized devices to a COV system or network such as personal computers, laptops, or hand held devices.
4. Prohibit the use of copyrighted and licensed materials on COV systems unless the COV owns the materials or COV has otherwise complied with intellectual property laws governing the materials.
5. Prohibit the transmission of unencrypted sensitive data over the Internet.
6. Include acceptable use in the Agency's IT security training program.
7. Require documentation of IT system users' acceptance of the Agency's Acceptable Use Policy before, or as soon as practicable after, gaining access to Agency IT systems.

## **9. THREAT MANAGEMENT**

### **9.1 Purpose**

Threat Management delineates the steps necessary to protect COV IT systems and data by preparing for and responding to IT security incidents. This component of the COV IT Security Program defines requirements in the following three areas:

- Threat Detection
- Incident Handling
- Security Monitoring and Logging

### **9.2 Threat Detection**

#### **9.2.1 Purpose**

Threat Detection requirements identify the practices for implementing intrusion detection and prevention.

#### **9.2.2 Requirements**

Each Agency shall or shall require that its service provider document threat detection practices that include the following components, at a minimum:

1. Designate an individual responsible for the Agency's threat detection program, including planning, development, acquisition, implementation, testing, training, and maintenance.
2. Require threat detection training for appropriate personnel, as practicable and necessary.
3. Conduct Intrusion Detection Systems (IDS) and Intrusion Prevention System (IPS) log reviews to detect new attack patterns as quickly as practicable.
4. Develop and implement required mitigation measures based on the results of IDS and IPS log reviews.
5. Maintain regular communication with security research and coordination organizations, such as US CERT, to obtain information about new attack types, vulnerabilities, and mitigation measures.

### **9.3 Incident Handling**

#### **9.3.1 Purpose**

Incident Handling requirements identify the steps necessary to respond to suspected or known breaches to IT security safeguards.

#### **9.3.2 Requirements**

Each Agency shall or shall require that its service provider document incident handling practices that include the following components, at a minimum:

1. Designate an Incident Response Team that includes personnel with appropriate expertise for responding to cyber attacks.

2. Identify controls to deter and defend against cyber attacks to best minimize loss or theft of information and disruption of services.
3. Implement proactive measures based on cyber attacks to defend against new forms of cyber attacks.
4. Establish incident categorization and prioritization based on the immediate and potential adverse effect of the incident and the sensitivity of affected IT systems and data.
5. Identify immediate mitigation procedures, including specific instructions, based on incident categorization level, on whether or not to shut down or disconnect affected IT systems.
6. Establish a reporting process for IT security incidents in accordance with §2.2-603(F) of the *Code of Virginia* so as to report “to the Chief Information Officer within 24 hours from when the department discovered or should have discovered their occurrence,” “all known incidents that threaten the security of the Commonwealth's databases and data communications resulting in exposure of data protected by federal or state laws, or other incidents compromising the security of the Commonwealth's information technology systems with the potential to cause major disruption to normal agency activities.”
7. Establish requirements for internal Agency IT security incident recording and reporting requirements, including a template for the incident report.
10. Establish procedures for incident investigation, preservation of evidence, and forensic analysis.
11. Require specialized incident response training as part of role-based security training programs for appropriate Agency personnel.
12. Report IT security incidents only through channels that have not been compromised.

## **9.4 IT Security Monitoring and Logging**

### **9.4.1 Purpose**

Security Monitoring and Logging requirements identify the steps necessary to monitor and record IT system activity.

### **9.4.2 Requirements**

Commensurate with sensitivity and risk, each Agency shall, or shall require that its service provider, document security monitoring and logging practices that include the following components, at a minimum:

1. Designate individuals responsible for the development and implementation of logging capabilities, as well as detailed procedures for reviewing and administering the logs.
2. Enable logging on all IT systems.
3. Monitor event logs in real time, correlate information with other automated tools, identifying suspicious activities, and provide alert notifications.
4. Document standards that specify the type of actions the program should take when a suspicious or apparent malicious activity is taking place.



**Example:** Possible actions include stopping the event, shutting down the system, and alerting appropriate staff.

**Note:** Multiple actions may be warranted and advisable, based on sensitivity and risk.

## **10. IT ASSET MANAGEMENT**

### **10.1 Purpose**

IT Asset Management delineates the steps necessary to protect COV IT systems and data by managing the IT assets themselves in a planned, organized, and secure fashion. This component of the COV IT Security Program defines requirements in the following three areas:

- IT Asset Control
- Software License Management
- Configuration Management and Change Control

### **10.2 IT Asset Control**

#### **10.2.1 Purpose**

IT Asset Control requirements identify the steps necessary to control and collect information about IT assets.

#### **10.2.2 Requirements**

Commensurate with sensitivity and risk, each Agency shall or shall require that its service provider document inventory management practices that address the following components, at a minimum:

1. Identify whether COV IT assets may be removed from premises that house COV IT systems and data, and if so, identify the controls over such removal.
2. Identify whether personal IT assets are allowed onto premises that house COV IT systems and data, and if so, identify the controls necessary to protect these systems and data.
3. Remove data from IT assets prior to disposal in accordance with the *COV Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard* (ITRM Standard SEC2003-02.1).

### **10.3 Software License Management**

#### **10.3.1 Purpose**

Software License Management requirements identify the steps necessary to protect against use of computer software in violation of applicable laws.

#### **10.3.2 Requirements**

Each Agency shall or shall require that its service provider document software license management practices that address the following components, at a minimum:

1. Require the use only of Agency approved software on COV IT systems.
2. Assess periodically whether all software is used in accordance with license agreements.

### **10.4 Configuration Management and Change Control**

#### **10.4.1 Purpose**

Configuration Management and Change Control requirements identify the steps necessary to document and monitor the configuration of IT systems, and to control changes to these items during

their lifecycles. While the full extent of Configuration Management and Change Control is beyond the scope of this document, Agencies are advised to institute structured practices in this area, based on industry standard frameworks such as the IT Infrastructure Library (ITIL) ([www.itil.co.uk](http://www.itil.co.uk)) or Control Objectives for Information and related Technology (COBIT)([www.isaca.org](http://www.isaca.org)), among others.

#### **10.4.3 Requirements**

Each Agency shall, or shall require that its service provider, document configuration management and change control practices so that changes to the IT environment do not compromise IT security controls.

*This section intentionally left Blank*

## GLOSSARY OF IT SECURITY DEFINITIONS

*Academic Instruction and Research Systems:* Those systems used by institutions of higher education for the purpose of providing instruction to students and/or by students and/or faculty for the purpose of conducting research.

*Access:* The ability or permission to enter or pass through an area or to view, change, or communicate with an IT system.

*Access Controls:* A set of procedures performed by hardware, software, and administrators to monitor access, identify all IT system users requesting access, record access attempts, and prevent unauthorized access to IT systems and data. Account an established relationship between a user and an IT system.

*Accountability:* The association of each log-on ID with one and only one user, so that the user can always be tracked while using an IT system, providing the ability to know which user performed what system activities.

*Agency Head:* The chief executive officer of a department established in the executive branch of the Commonwealth of Virginia.

*Alert:* Advance notification that an emergency or disaster situation may occur.

*Alternate Site:* A location used to conduct critical business functions in the event that access to the primary facility is denied or the primary facility has been so damaged as to be unusable.

*Application:* A computer program or set of programs that meet a defined set of business needs. See also *Application System*.

*Application System:* An interconnected set of IT resources under the same direct management control that meets a defined set of business needs. See also *Application*, *Support System*, and *Information Technology (IT) System*.

*Asset:* Any software, data, hardware, administrative, physical, communications, or personnel resource.

*Attack:* An attempt to bypass security controls on an IT system. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the IT system and the effectiveness of existing countermeasures.

*Audit:* An independent review and examination of records and activities to test for adequacy of controls, measure compliance with established policies and operational procedures, and recommend changes to controls, policies, or procedures.

*Authenticate:* To determine that something is genuine. To reliably determine the identity of a communicating party or device.

*Authentication:* The process of verifying the identity of a station, originator, or individual to determine the right to access specific types of data. In addition, a measure designed to protect against fraudulent transmission by verifying the validity of a transmission, message, station, or originator. During the process, the user enters a name or account number (identification) and password (authentication).

*Authenticator:* The material or credential used to create or implement authentication bindings such as a password, PIN number, token seed, smart card seed, etc.

*Authorization:* Granting the right of access to a user, program, or process. The privileges granted to an individual by a designated official to access data, based upon the individual's job, clearance, and need to know.

*Availability:* The computer security characteristic that addresses requirements for IT systems and data to be operational in support of essential business functions and that measures the sensitivity of IT systems and data to unexpected outages.

*Backup:* The process of producing a reserve copy of software or electronic files as a precaution in case the primary copy is damaged or lost.

*Baseline Security Configuration:* The minimum set of security controls that must be implemented on all IT systems of a particular type.

*Business Function:* A collection of related structural activities that produce something of value to the organization, its stakeholders or its customers. See also *Essential Business Function*.

*Business Impact Analysis (BIA):* The process of determining the potential consequences of a disruption or degradation of business functions.

*Chain of Custody:* Documentation that is sufficient to prove continuous and unbroken possession of a confiscated IT system.

*Change Control:* A management process to provide control and traceability for all changes made to an application system or IT system.

*Chief Information Officer of the Commonwealth (CIO):* The CIO oversees the operation of the Virginia Information Technologies Agency (VITA) and, under the direction and control of the Virginia Information Technology Investment Board (the Board), exercises the powers and performs the duties conferred or imposed upon him by law and performs such other duties as may be required by the Board.

*Chief Information Security Officer of the Commonwealth (CISO):* The CISO is the senior management official designated by the CIO of the Commonwealth to develop Information Security policies, procedures, and standards to protect the confidentiality, integrity, and availability of COV IT systems and data.

*Commonwealth of Virginia (COV):* The Executive Branch of the government of the Commonwealth of Virginia, or its Agencies or departments.

*Computer Emergency Response Team Coordination Center (CERT/CC):* a center of Internet security expertise, located at the Software Engineering Institute at Carnegie Mellon University that studies Internet security vulnerabilities, researches long-term changes in networked systems, and develops information and training to assist the CERTs of other organizations. See also *Incident Response Team* and *United States Computer Emergency Response Team (US-CERT)*.

*Confidentiality:* The computer security characteristic that addresses requirements that data is disclosed only to those authorized to access it, and that measures the sensitivity of data to unauthorized disclosure.

*Configuration Management:* A formal process for authorizing and tracking all changes to both hardware and software of an IT system during its life cycle.

*Continuity of Operations Planning:* The process of developing plans and procedures to continue the performance of essential business functions in the event of a business interruption or threat of interruption.

*Continuity of Operations Plan (COOP):* A set of documented procedures developed to provide for the continuance of essential business functions during an emergency.

*Control Objectives for Information and related Technology (COBIT):* A framework of best practices (framework) for IT management that provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control.

*Council on Technology Services (COTS):* An advisory council that assists in the development of a blueprint for state government IT planning and decision-making. The Council advises the Chief Information Officer of the Commonwealth on the services provided by the Virginia Information Technologies Agency (VITA) and the development and use of applications in state agencies and public institutions of higher education.

*Countermeasure:* An action, device, procedure, technique, or other measure that reduces vulnerability or the impact of a threat to an IT system.

*Credential:* Information passed from one entity to another that is used to establish the sending entity's access rights.

*Data:* Data consists of a series of facts or statements that may have been collected, stored, processed and/or manipulated but have not been organized or placed into context. When data is organized, it becomes information. Information can be processed and used to draw generalized conclusions or knowledge.

*Database:* A database is a collection of data organized into interrelated tables and specifications of data objects.

*Data Classification:* A process of categorizing data according to its sensitivity.

*Data Communications:* Data Communications includes the equipment and telecommunications facilities that transmit, receive, and validate Commonwealth of Virginia (COV) data between and among computer systems, including the hardware, software, interfaces, and protocols required for the reliable movement of this information. As used in this document, Data Communications is included in the definition of government database, herein.

*Data Custodian:* An individual or organization in physical or logical possession of data for Data Owners. Data Custodians are responsible for protecting the data in their possession from unauthorized access, alteration, destruction, or usage and for providing and administering general controls, such as back-up and recovery systems.

*Data Owner:* An Agency Manager responsible for the policy and practice decisions regarding data. For business data, the individual may be called a business owner of the data.

*Data Security:* Data Security refers to those practices, technologies, and/or services used to apply security appropriately to data.

*Disaster Recovery Plan (DRP):* A set of documented procedures that identify the steps to restore essential business functions on a schedule that supports Agency mission requirements.

*Data Storage Media:* A device used to store IT data. Examples of data storage media include floppy disks, fixed disks, CD-ROMs, and USB flash drives.

*Encryption:* A means of scrambling data so it cannot be read without the appropriate decryption methodology.

*Essential Business Function:* A business function is essential if disruption or degradation of the function prevents the Agency from performing its mission as described in the Agency mission statement.

*Evaluation:* Investigative and test procedures used in the analysis of security mechanisms to determine their effectiveness and to support or refute specific system weaknesses.

*Extranet:* A trusted network; used by COV to connect to a third-party provider.

*Federal Information Security Management Act (FISMA):* Federal legislation whose primary purpose is to provide a comprehensive framework for IT security controls in Federal agencies.

*Firewall:* Traffic-controlling gateway that controls access, traffic, and services between two networks or network segments, one trusted and the other untrusted.

*Function:* A purpose, process, or role.

*Government Database:* For the purposes of this document, the term “government database” includes both databases that contain COV data and data communications that transport COV data. This definition applies irrespective of whether the COV information is in a physical database structure maintained by COV or a third-party provider. However, this definition does not include databases within Agencies that have been determined by the Agencies themselves to be non-governmental. See also *Database* and *Data Communications*.

*Group:* A named collection of IT system users; created for convenience when stating authorization policy.

*Harden:* The process of implementing software, hardware, or physical security controls to mitigate risk associated with COV infrastructure and/or sensitive IT systems and data.

*High Availability:* A requirement that the IT system is continuously available, has a low threshold for down time, or both.

*Identification:* The process of associating a user with a unique user ID or login ID.

*Incident Response Capability (IRC):* The follow-up to an unplanned event such as a hardware or software failure or attack against a computer or network.

*Incident Response Team:* An organization within an Agency constituted to monitor IT security threats and prepare for and respond to cyber attacks. See also *Computer Emergency Response Team Coordination Center (CERT/CC)* and *United States Computer Emergency Response Team (US-CERT)*.

*Individual Accountability:* The process of associating one and only one IT system user or IT system (such as a workstation or terminal) with any actions performed.

*Information Security Officer (ISO):* The individual who is responsible for the development, implementation, oversight, and maintenance of the Agency’s IT security program.

*Information Technology (IT):* Telecommunications, automated data processing, databases, the Internet, management information systems, and related information, equipment, goods, and services.

*Information Technology (IT) Infrastructure Library (ITIL):* A framework of best practice processes designed to

facilitate the delivery of high quality information technology (IT) services.

*Information Technology (IT) Security:* The protection afforded to IT systems and data in order to preserve their availability, integrity, and confidentiality.

*Information Technology (IT) Security Architecture:* The logical and physical security infrastructure made up of products, functions, locations, resources, protocols, formats, operational sequences, administrative and technical security controls, etc., designed to provide the appropriate level of protection for IT systems and data.

*Information Technology (IT) Security Audit:* An independent review and examination of an IT system's policy, records, and activities. The purpose of the IT security audit is to assess the adequacy of IT system controls and compliance with established IT security policy and procedures.

*Information Technology (IT) Security Auditor:* CISO personnel, Agency Internal Auditors, the Auditor of Public Accounts, or a private firm that, in the judgment of the Agency, has the experience and expertise required to perform IT security audits.

*Information Technology (IT) Security Breach:* The violation of an explicit or implied security policy that compromises the integrity, availability, or confidentiality of an IT system.

*Information Technology (IT) Security Controls:* The protection mechanisms prescribed to meet the security requirements specified for an IT system. These mechanisms may include but are not necessarily limited to: hardware and software security features; operating procedures, authorization and accountability access and distribution practices; management constraints; personnel security; and environmental and physical safeguards, structures, and devices. Also called IT security safeguards and countermeasures.

*Information Technology (IT) Security Incident:* An adverse event or situation, whether intentional or accidental, that poses a threat to the integrity, availability, or confidentiality of an IT system. A security incident includes an attempt to violate an explicit or implied security policy.

*Information Technology (IT) Security Logging:* Chronological recording of system activities sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to its final results.

*Information Technology (IT) Security Requirements:* The types and levels of protection necessary to adequately secure an IT system.

*Information Technology (IT) Security Safeguards:* See *Information Technology (IT) Security Controls*.

*Information Technology (IT) System:* An interconnected set of IT resources under the same direct management control. See also *Application System* and *Support System*.

*Information Technology (IT) System Users:* As used in this document, a term that includes COV employees, contractors, vendors, third-party providers, and any other authorized users of COV IT systems, applications, telecommunication networks, data, and related resources. It excludes customers whose only access is through publicly available services, such as public COV Web sites.

*Insecure:* Unprotected, as an IT system.

*Integrity:* The computer security characteristic that addresses the accuracy and completeness of IT systems and data, and that measures the sensitivity of IT systems and data to unauthorized or unexpected modification.

*Integrity Check:* Validates that a message has not been altered since it was generated by a legitimate source (based on representation of information as numbers and mathematic manipulation of those numbers).

*Internet:* An external worldwide public data network using Internet protocols to which COV can establish connections. COV has no control over the Internet and cannot guarantee the confidentiality, integrity, or availability of its communications.

*Intranet:* A trusted multi-function (data, voice, video, image, facsimile, etc.) private digital network using Internet protocols, which can be developed, operated and maintained for the conduct of COV business.

*Intrusion Detection:* A method of monitoring traffic on the network to detect break-ins or break-in attempts, either manually or via software expert systems.

*Intrusion Detection Systems (IDS):* Software that detects an attack on a network or computer system. A Network IDS (NIDS) is designed to support multiple hosts, whereas a Host IDS (HIDS) is set up to detect illegal actions within the host. Most IDS programs typically use signatures of known cracker attempts to signal an alert. Others look for deviations of the normal routine as indications of an attack.

*Intrusion Prevention Systems (IPS):* Software that prevents an attack on a network or computer system. An IPS is a significant step beyond an IDS (intrusion detection system), because it stops the attack from damaging or retrieving data. Whereas an IDS passively monitors traffic by sniffing packets off of a switch port, an IPS resides inline like a firewall, intercepting and forwarding packets. It can thus block attacks in real time.

*ISO/IEC 17799:* An IT security standard published in 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It provides best practice recommendations on IT security management for use by those who are responsible for initiating, implementing or maintaining information security management systems.

*Key:* A sequence of data used in cryptography to encrypt or decrypt information. The keys must be known or deduced to forge a digital signature or decrypt an encrypted message.

*Key Escrow:* The process of storing the encryption key with a third-party trustee to allow the recovery of encrypted text.

*Least Privilege:* The minimum level of data, functions, and capabilities necessary to perform a user's duties. Application of this principle limits the damage that can result from accident, error, or unauthorized use of an IT system.

*Log:* To record an action.

*Log File:* A chronological record of operational and security-related events that have occurred.

*Logon ID:* An identification code (normally a group of numbers, letters, and special characters) assigned to a particular user that identifies the user to the IT system.

*Malicious Code:* Harmful code (such as viruses and worms) introduced into a program or file for the purpose of contaminating, damaging, or destroying IT systems and/or data. Malicious code includes viruses (boot sector, file infector, multipartite, link, stealth, macro, e-mail, etc.), Trojan horses, trap doors, worms, spyware, and counterfeit computer instructions (executables).

*Malicious Software:* See Malicious Code.

*Mission Critical Facilities:* The data center's physical surroundings as well as data processing equipment inside and the systems supporting them that need to be secured to achieve the availability goals of the system function.

*Monitoring:* Listening, viewing, or recording digital transmissions, electromagnetic radiation, sound, and visual signals.

*Non-sensitive Data:* Data of which the compromise with respect to confidentiality, integrity, and/or availability could not adversely affect COV interests, the conduct of Agency programs, or the privacy to which individuals are entitled.

*Off-site Storage:* The process of storing vital records in a facility that is physically remote from the primary site. To qualify as off-site, the facility should be at least 500 yards from the primary site and offer environmental and physical access protection.

*Operational Risk:* Any risk that is not market risk or credit risk related. This includes the risk of loss from events related to technology and infrastructure failure, from business interruptions, from staff related problems and from external events such as regulatory changes. Examples of operational risk include: technology failure; business premises becoming unavailable; inadequate document retention or record-keeping; poor management; lack of supervision, accountability and control; errors in financial



models and reports; attempts to conceal losses or make personal gains (rogue trading); and third-party fraud.

*Out-of-Band Communications:* A way to send data (e.g., files) outside the context of normal communications. Out of band communications provide a secondary communications channel for emergencies and/or redundancy.

*Password:* A unique string of characters that, in conjunction with a logon ID, authenticates a user's identity.

*Personal Digital Assistant (PDA):* A digital device, which can include the functionality of a computer, a cellular telephone, a music player and a camera

*Personal Identification Number (PIN):* A short sequence of digits used as a password.

*Personnel:* All COV employees, contractors, and subcontractors, both permanent and temporary.

*Phishing:* A form of criminal activity characterized by attempts to acquire sensitive information fraudulently, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication.

*Plain Text Message:* A message sent without encryption.

*Privacy:* The rights and desires of an individual to limit the disclosure of individual information.

*Privacy Officer:* The privacy officer, if required by statute (such as HIPPA) provides guidance on the requirements of state and federal Privacy laws; disclosure of and access to sensitive data; and security and protection requirements in conjunction with the IT system when there is some overlap among sensitivity, disclosure, privacy, and security issues.

*Proprietary Information:* Specific and unique material and information relating to or associated with a company's products, business, or activities. This information must have been developed for or by the company and must not be available freely from another source.

*Recovery:* Activities beyond the initial crisis period of an emergency or disaster that are designed to return IT systems and/or data to normal operating status.

*Repudiation:* Denial that one did or said something.

*Residual Risk:* The portion of risk that remains after security measures have been applied.

*Restoration:* Activities designed to return damaged facilities and equipment to an operational status.

*Restricted Data:* Data which has limited availability; based on COV regulations.

*Risk:* The possibility of loss or injury based on the likelihood that an event will occur and the amount of harm that could result.

*Risk Assessment (RA):* The process of identifying the vulnerabilities, threats, likelihood of occurrence, potential loss or impact, and theoretical effectiveness of security measures. Results are used to evaluate the level of risk and to develop security requirements and specifications.

*Risk Mitigation:* The continuous process of minimizing risk by applying security measures commensurate with sensitivity and risk.

*Roles and Responsibility:* Roles represent a distinct set of operations and responsibilities required to perform some particular function that an individual may be assigned. Roles may differ from the individual's business title. This document contains the roles and responsibilities associated with implementing IT security.

*Recovery Time Objective (RTO):* The amount of time targeted for the recovery of a business function or resource after a disaster occurs.

*Secure:* A state that complies with the level of security controls that have been determined to provide adequate protection against adverse contingencies.

*Sensitive Data:* Any data of which the compromise with respect to confidentiality, integrity, and/or availability could adversely affect COV interests, the conduct of Agency programs, or the privacy to which individuals are entitled.

*Sensitive IT Systems:* COV IT systems that store, process, or transmit sensitive data.

*Sensitivity Classification:* The process of determining whether and to what degree IT systems and data are sensitive.

*Separation of Duties:* Assignment of responsibilities such that no one individual or function has control of an entire process. Implied in this definition is the concept that no one person should have complete control. Separation of duties is a technique for maintaining and monitoring accountability and responsibility for IT systems and data.

*Shared Accounts:* A logon ID or account utilized by more than one entity.

*Sign:* The process of using a private key to generate a digital signature as a means of proving generation or approval of a message.

*Signature:* A quantity associated with a message that only someone with knowledge of a user's private key could have generated but which can be verified through knowledge of the user's public key.

*Spyware:* A category of malicious software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user. While the term taken literally suggests software that surreptitiously monitors the user, it has come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.

*State:* See *Commonwealth of Virginia (COV)*.

*Support System:* An interconnected set of IT resources under the same direct management control that shares common functionality and provides services to other systems. See also *Application System* and *Information Technology (IT) System*.

*System.* See *Information Technology (IT) System*

*System Administrator:* An analyst, engineer, or consultant who implements, manages, and/or operates a system at the direction of the System Owner, Data Owner, and/or Data Custodian.

*System Owner:* An Agency Manager responsible for the operation and maintenance of an Agency IT system.

*Technology Strategy and Solutions (TSS):* A directorate within VITA; the publisher of all VITA external and internal policies, standards, and guidelines. TSS develops architectural standards and the accompanying policies and procedures for the enterprise, and advises the CIO on architectural standards and exceptions. It also tracks emerging trends and best practices across the spectrum of technologies, including hardware, operating systems, networking and communications, security, and software applications.

*Third-Party Provider:* A company or individual that supplies IT equipment, systems, or services to COV Agencies.

*Threat:* Any circumstance or event (human, physical, or environmental) with the potential to cause harm to an IT system in the form of destruction, disclosure, adverse modification of data, and/or denial of service by exploiting vulnerability.

*Token:* A small tangible object that contains a built-in microprocessor utilized to store and process information for authentication.

*Trojan horse:* A malicious program that is disguised as or embedded within legitimate software. The term is derived from the classical myth of the Trojan Horse. Trojan horse programs may look useful or interesting to an unsuspecting IT system user, but are actually harmful when executed.

*Trusted:* Recognized automatically as reliable, truthful, and accurate, without continual validation or testing.

*United States Computer Emergency Response Team (US-CERT):* A partnership between the Department of Homeland security and the public and private sectors, intended to coordinate the response to IT security threats from the Internet. As such it releases information about current IT security issues, vulnerabilities and exploits as Cyber Security Alerts, and works with software vendors to create patches for IT security vulnerabilities. See also *Computer Emergency Response Team Coordination Center (CERT/CC)* and *Incident Response Team*.

*Universal Serial Bus (USB):* A standard for connecting devices.

*Untrusted:* Characterized by absence of trusted status. Assumed to be unreliable, untruthful, and inaccurate unless proven otherwise.

*USB Flash Drive:* A small, lightweight, removable and rewritable data storage device.

*User ID:* A unique symbol or character string that is used by an IT system to identify a specific user. See Logon ID.

*Virginia Department of Emergency Management (VDEM):* A COV department that protects the lives and property of Virginia's citizens from emergencies and disasters by coordinating the state's emergency preparedness, mitigation, response, and recovery efforts

*Version Control:* A management process to traceability of updates to operating systems and supporting software.

*Virus:* See Malicious Code.

*Virginia Information Technologies Agency (VITA):* VITA is the consolidated, centralized IT organization for COV.

*Vital Record:* A document, regardless of media, which, if damaged or destroyed, would disrupt business operations.

*Vulnerability:* A condition or weakness in security procedures, technical controls, or operational processes that exposes the system to loss or harm.

*Workstation:* A terminal, computer, or other discrete resource that allows personnel to access and use IT resources.

## IT SECURITY ACRONYMS

AITR: Agency Information Technology Representative

ANSI: American National Standards Institute

BIA: Business Impact Analysis

CAP: Corrective Action Plan

CIO: Chief Information Officer

CISO: Chief Information Security Officer

COOP: Continuity of Operations Plan

COPPA: Children's Online Privacy Protection Act

COTS: Council on Technology Services

DHRM: Department of Human Resource Management

DRP: Disaster Recovery Plan

FIPS: Federal Information Processing Standards

FISMA: Federal Information Security Management Act

FTP: File Transfer Protocol

HIPAA: Health Insurance Portability and Accountability Act

IDS: Intrusion Detection Systems

IPS: Intrusion Prevention Systems

IRC: Incident Response Capability

ISA: Interconnection Security Agreement

ISO: Information Security Officer

ITRM: Information Technology Resource Management

MOU: Memorandum of Understanding

OMB: Office of Management and Budget

PDA: Personal Digital Assistant

PIA: Privacy Impact Assessment

PII: Personally Identifiable Information

PIN: Personal Identification Number

RA: Risk Assessment

RBD: Risk-Based Decisions

RTO: Recovery Time Objective

SLA: Service Level Agreement

SDLC: Systems Development Life Cycle

SNMP: Simple Network Management Protocol

SOP: Standard Operating Procedure

SSID: Service Set Identifier

SSP: Security Program Plan

ST&E: Security Test & Evaluation

TSS: Technology Strategy and Solutions Directorate (VITA)

USCERT: Computer Emergency Response Team

VDEM: Virginia Department of Emergency Management

VITA: Virginia Information Technologies Agency

## **APPENDIX – IT SECURITY POLICY AND STANDARD EXCEPTION REQUEST FORM**

**The form an Agency must submit to request an exception to any requirement of this *Standard* and the related *IT Security Policy* is on the following page.**

## IT Security Management Policy & Standard Exception Request Form

Date of Request: \_\_\_\_\_

Requester: \_\_\_\_\_ Agency Name: \_\_\_\_\_

IT Security Policy or Standard to which an exception is requested:

\_\_\_\_\_

In each case, the Agency requesting the exception must:

1. Provide the **Business or Technical Justification** for not implementing the Standard:
2. Describe the scope and extent of the exception:
3. Identify the safeguards which will be implemented to mitigate risks associated with the exception:
4. Define the specific duration of the exception (not to exceed six (6) months):

Approved \_\_\_\_\_ Date \_\_\_\_\_  
Agency Head

### Chief Information Security Officer of the Commonwealth (CISO) Use Only

Approved \_\_\_\_\_ Denied \_\_\_\_\_ Comments:

\_\_\_\_\_  
CISO Date

### Agency Request for Appeal Use Only

Approved \_\_\_\_\_ Comments:

\_\_\_\_\_  
Agency Head Date

### Chief Information Officer of the Commonwealth (CIO) Office Use Only (Appeal)

Appeal  
Approved \_\_\_\_\_ Appeal  
Denied \_\_\_\_\_ Comments:

\_\_\_\_\_  
CIO Date

